ADCO AI LLC

Data Protection Policy

ADCO AI LLC requires personal information to be handled lawfully, fairly, securely, and for defined purposes. This policy establishes the data protection standards that ADCO AI LLC and its participating subsidiaries and affiliated entities must apply across business administration and authorized service delivery.

01 Purpose and application

This policy applies to personnel, contractors, and participating ADCO entities handling personal information through websites, recruitment, workforce administration, commercial relationships, research, data collection, annotation, AI evaluation, human review, and other authorized operations. Relevant requirements must also be reflected in arrangements with providers processing information for ADCO.

Personal information includes information identifying or reasonably relating to an individual, whether in text, images, audio, video, metadata, annotations, or derived results. Pseudonymized information remains personal information when it can be linked back to an individual. Confidential client information also remains subject to its contractual protections whether or not it is personal information.

This policy sets operating requirements. The Privacy Policy and specific applicant, workforce, or participant notices explain processing to individuals. Client agreements define engagement obligations. None of these documents permits unlawful processing, overrides mandatory rights, or replaces a required data processing agreement or assessment.

02 Accountability and responsibilities

Leadership must assign responsibility for the privacy program, provide appropriate resources, and review material risks and corrective actions. The designated privacy function coordinates notices, legal-basis assessments, requests, transfer questions, and regulatory matters. Any legally required data protection officer or representative must be appointed with the authority, independence, and access required for that role.

Business and project owners must define purposes, data flows, access, vendors, retention, and client instructions before processing begins. Security and system owners must implement the required safeguards and support incident response. Recruitment and workforce managers must protect applicant and personnel records according to their specific purpose.

Personnel must use information only within their authorization, complete required training, protect credentials, and promptly report mistakes or suspected misuse. Responsibility cannot be avoided by delegating a task to a provider. An unresolved legal, privacy, or security concern must be escalated before the affected processing continues.

03 Core processing principles

Each activity must have a lawful and transparent purpose. Collection and access must be limited to information reasonably necessary for that purpose. Individuals must not be misled about how their information will be used, and information obtained for one purpose must not be repurposed incompatibly without the necessary assessment and legal authority.

Information must be reasonably accurate for its use, with routes to correct material errors. Retention must have a defined purpose and endpoint or meaningful criteria. Appropriate confidentiality, integrity, availability, and security protections must apply throughout collection, use, disclosure, storage, and disposal.

Owners must retain proportionate evidence of decisions and safeguards. Privacy controls must be considered when a process is designed, rather than added only after collection. Default settings must minimize unnecessary collection, sharing, access, and retention.

04 Processing roles and client instructions

ADCO acts as a controller when it determines the purposes and means of processing for its own business. It acts as a processor, service provider, contractor, or subprocessor where it processes personal information on a client's behalf. Actual activities determine the role; a contract label alone is insufficient. Jointly determined activities require the responsibilities and transparency required by applicable law.

Before client processing begins, the applicable arrangements must identify the parties and roles, purpose, duration, information and individual categories, authorized systems, locations, access, providers, security requirements, retention, and contacts. Required processing terms must address documented instructions, confidentiality, safeguards, subprocessing, individual rights, incident and assessment assistance, return or deletion, and audit or compliance information.

Personnel must follow documented client instructions. If an instruction appears unlawful, ADCO must promptly inform the appropriate client contact and escalate the issue. No one may proceed merely to meet a deadline. A legally compelled departure requires appropriate review and client notice where required and permitted.

05 Lawful grounds, notices, and consent

Where a legal basis is required, the responsible owner must identify and document the basis for each purpose before processing. Contractual necessity is limited to what is necessary for the relevant individual contract. Reliance on legitimate interests requires assessment of purpose, necessity, and effects on individuals. Legal-obligation processing must identify the relevant obligation.

Consent must meet applicable requirements for an informed, specific, freely given, and unambiguous choice. Required explicit consent must be obtained where applicable. Records must show the relevant notice, choice, and withdrawal route. Withdrawal must be respected for future consent-based processing, without treating another basis as an automatic substitute.

Collection notices must identify the responsible entity and explain relevant categories, sources, purposes, bases, recipients, transfers, retention, rights, and contacts. Required or optional fields and consequences must be clear. Indirect collection requires timely notice unless a lawful exception is documented. Accepting website terms is not universal permission for tracking, recruitment reuse, or dataset distribution.

06 Information records and risk assessment

Owners must maintain an accurate inventory of relevant processing activities and data flows. Records must identify responsible entities and contacts, purposes, roles, categories of individuals and information, systems, recipients, processing countries, transfer safeguards, retention, and a general description of security measures. Applicable lawful-basis and consent records must be linked to the activity.

New or materially changed processing must undergo a proportionate privacy risk review. High-risk activities require a data protection impact assessment when applicable, before implementation. The review must consider necessity, proportionality, foreseeable harm, affected groups, alternatives, safeguards, remaining risk, and assigned actions.

Sensitive datasets, monitoring, significant automated decisions, large-scale profiling, new AI uses, and information about children require particular scrutiny. Required regulatory consultation must occur before processing that retains unmitigated high risk. Client-controlled assessments receive the assistance required by the engagement and applicable law.

07 Sensitive information and vulnerable individuals

Sensitive information requires an authorized purpose and any additional legal condition, assessment, consent, or documentation required for its category. Access must be more restrictive where the risk warrants it. General inquiry or application forms must not be used to solicit unnecessary health records, identity documents, financial details, or other sensitive material.

Protected health information is not accepted by default. Any proposed health-data engagement requires an applicability review, required agreements, appropriate systems and providers, risk assessment, and authorization before access. Full payment-card credentials must not be placed in public forms, ordinary project files, email, or chat; any permitted card collection must use an approved payment process.

Projects involving minors require an age and rights assessment, lawful permissions, appropriate notices, and additional protections before collection. Participation or data access must not exploit dependency, limited understanding, or a power imbalance. A photograph or recording is not automatically biometric identification data, but remains protected when identifiable.

08 Access, workforce handling, and safeguards

Access must be approved for a defined task, limited to the minimum needed, and linked to an identifiable authorized person. Our standards require individual accounts, appropriate authentication including multi-factor authentication where supported, separation of privileged access, and prompt access adjustment when responsibilities or employment change.

Personnel must accept applicable confidentiality obligations and receive role-appropriate instruction before access. Refresher guidance must address material changes and identified weaknesses. Approved devices, systems, transfer channels, and work locations must be used. Personal accounts, public sharing links for confidential client information, and unapproved tools are prohibited. Local copies and removable media require specific authorization and adequate safeguards under the engagement's rules.

Safeguards must address encryption appropriate to storage and transmission risks, access review, system maintenance, logging, secure configuration, physical protection, backup handling, and secure disposal. Project owners must verify required safeguards before activation. A public policy statement is not a substitute for implementing or evidencing a required control.

09 Human review, AI use, and derived information

Human reviewers may access personal information only where needed for the authorized task. Instructions must define permitted viewing, copying, annotation, quality review, and escalation. Screenshots, demonstrations, training examples, and internal research must not expose client information outside the authorized purpose.

Client personal information must not be used for ADCO's independent model training, unrelated datasets, advertising, or licensing. AI training or evaluation commissioned by a client is limited to that engagement. Submission to public AI services, unapproved tools, personal accounts, or providers with incompatible retention or training terms is prohibited.

Any approved AI-assisted use requires review of purpose, contractual authorization, provider terms, disclosure, retention, location, security, and applicable rights. Annotations, embeddings, scores, and other derived information remain protected where they identify or can be linked to individuals. Claims that information is anonymous require an assessment of realistic reidentification risks and safeguards against unauthorized reidentification.

10 Participants and significant automated decisions

Direct collection for a dataset or participant project requires a specific notice describing the responsible entity, information, purpose, recipients, relevant training or evaluation uses, retention, and rights. Any licensing or distribution of identifiable contributions requires the necessary legal authority and clear disclosure. General participation consent must not be stretched to cover undisclosed future uses.

Profiling and solely automated decisions with legal or similarly significant effects require a jurisdiction-specific assessment, permitted grounds, meaningful transparency, and applicable safeguards before use. Required human intervention, challenge, and review procedures must be effective. A person merely confirming an automated output does not necessarily constitute meaningful review. Automated tools supporting personnel administration must not replace accountable human decisions about hiring, termination, discipline, or pay changes.

Withdrawal and deletion requests must be assessed against the actual processing and applicable rights. Inclusion in a dataset or AI workflow does not automatically extinguish privacy rights. Any lawful limitation must be explained accurately.

11 Providers, affiliates, and other disclosures

Providers must undergo due diligence proportionate to their access and risk before receiving information. Review must address service necessity, security, confidentiality, permitted use, subprocessing, processing locations, incident reporting, assistance, retention, and deletion. Written terms must impose the protections required by the applicable relationship and law.

Client subprocessors require the specified prior authorization and change-notification process. Applicable data protection obligations must be passed down, and ADCO must retain the responsibility required by law and contract. A new vendor or corporate affiliate cannot receive client data solely because it is convenient.

Independent disclosures require a lawful purpose and limited scope. Requests from authorities must be reviewed for validity and necessity, with notice to the relevant client or individual where required and permitted. Provider and disclosure records must remain current, and material changes must trigger reassessment.

12 International access and transfers

Data-flow reviews must account for hosting, support, remote access, and onward transfers, including ADCO operations in the United States and Ethiopia. Client restrictions on locations and access remain binding. An overseas login may constitute a restricted transfer even when storage remains in another country.

Before a restricted transfer, the responsible owner must document the relevant entities, roles, countries, permitted mechanism, and necessary safeguards. Available mechanisms may include an applicable adequacy decision, approved contractual clauses, and a UK transfer agreement or addendum completed for the actual transfer.

Required transfer assessments and supplementary measures must address relevant risks, including government access and onward processing. Transfers must be reassessed following material changes. Where necessary protections cannot be provided, the affected transfer must not begin or must be suspended. Website use is not a substitute for a lawful mechanism.

13 Individual requests and complaints

Requests received through any recognized channel must be routed promptly to the privacy function and logged with applicable deadlines. The response process must establish the relevant entity and role, verify identity and authority only as necessary, locate records, evaluate exceptions, and provide an intelligible response through a suitable channel.

Applicable rights may include access, correction, deletion, restriction, portability, objection, withdrawal, opt-outs, and safeguards for significant automated decisions. Personnel must not impose prohibited verification, an unnecessary account requirement, or retaliation. Extensions and refusals require a lawful reason and appropriate explanation, including appeal or complaint routes where applicable.

For client-controlled information, ADCO must promptly refer the request to the client and provide required assistance without independently disclosing or deleting records contrary to lawful instructions. Requests and complaints may be sent to privacy@adcohq.com; a request to review a response may use 'Privacy Appeal' as its subject.

14 Retention, return, and secure disposal

Each activity must have documented retention periods or meaningful criteria linked to its purpose, legal obligations, and contractual requirements. Records must not be retained indefinitely for unspecified future use. Owners must review whether the purpose remains active and apply appropriate deletion, return, or genuine anonymization when it ends.

At the end of client processing, information must be returned or deleted according to the client's applicable choice and agreement, subject to lawful retention duties. Disposition and any required confirmation must cover relevant working copies and approved providers. Necessary legal holds must identify the records, reason, access restrictions, and review conditions.

Residual backups must remain protected from ordinary use and expire through the applicable lifecycle. Restoration must not silently reverse an applicable deletion; relevant restrictions and deletion instructions must be reapplied. Sensitive paper and electronic records require disposal that reasonably prevents reconstruction or unauthorized recovery.

15 Incidents and personal data breaches

Suspected loss, unauthorized access or disclosure, alteration, or destruction must be reported immediately through the designated incident route. Personnel must preserve relevant evidence and follow authorized containment instructions. Incidents must be assessed for affected information, individuals, systems, likely consequences, and legal or contractual obligations.

When ADCO acts as a processor, it must notify the responsible client without undue delay after becoming aware of a personal data breach and meet any additional contractual reporting requirements. Notification must not wait for a complete forensic investigation. Available facts may be provided in stages with appropriate updates.

When ADCO is the controller, the privacy function must assess regulatory and individual notification requirements and meet applicable deadlines. Where EU or UK rules require regulatory notice, it must be given without undue delay and, where feasible, within 72 hours of awareness; that period is not a universal waiting period or a replacement for earlier client duties. Decisions to notify or not notify, reasons, remediation, and lessons must be documented.

16 Assurance, enforcement, and review

Responsible owners must retain proportionate evidence of training, processing decisions, provider reviews, access controls, requests, incidents, and corrective actions. Leadership must periodically review the policy's effectiveness and reassess it following material legal, operational, or risk changes. Identified deficiencies require an owner, corrective action, and follow-up.

Client and regulatory reviews must receive the assistance and access required by law and agreement, with appropriate protection for other clients' information, credentials, personal data, and continuity. Statements about certifications or implemented controls must be supported by current evidence; the existence of this policy does not establish certification.

Policy breaches may result in access suspension, remediation, disciplinary action, or contractual remedies as appropriate and lawful. Any permitted exception requires documented risk review, authorization, compensating safeguards, and an expiry or reassessment point. No exception may waive law or binding client obligations. Privacy questions and concerns may be directed to ADCO AI LLC at privacy@adcohq.com.